Docket No.: RSW920010151US1 (7161-009U) **PATENT**

**IN THE UNITED STATES PATENT AND TRADEMARK OFFICE**
**BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES**

| | | |
|---|---|---|
| In re Application of | : | Customer Number: 46320 |
| Brian MARTIN | : | Confirmation Number: 1846 |
| Application No.: 09/944,996 | : | Group Art Unit: 2134 |
| Filed: August 31, 2001 | : | Examiner: L. Ha |

For: STATE MACHINE FOR ACCESSING A STEALTH FIREWALL

## APPEAL BRIEF

Mail Stop Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Sir:

This Supplemental Appeal Brief is submitted, pursuant to 37 C.F.R. § 41.39(b)(2), in support of the Notice of Appeal filed December 2, 2005, and in response to the Examiner reopening prosecution in the Office Action dated May 31, 2006, wherein Appellant appeals from the Examiner's rejection of claims 1-13.

## I. REAL PARTY IN INTEREST

This application is assigned to IBM Corporation by assignment recorded on August 31, 2001, at Reel 012146, Frame 0346.

## II. RELATED APPEALS AND INTERFERENCES

Appellant is unaware of any related appeals and interferences.

## III. STATUS OF CLAIMS

Claims 1-13 are pending in this Application. Of those, claims 1-13 have been three-times rejected, and it is from the multiple rejections of claims 1-13 that this Appeal is taken.

## IV. STATUS OF AMENDMENTS

The claims have not been amended subsequent to the imposition of the Final Office Action dated October 7, 2005, or the reopening of prosecution in the Office Action dated May 31, 2006.

## V. SUMMARY OF CLAIMED SUBJECT MATTER

Independent claims 1 and 7-13 are directed to stealth firewalls, methods, and machine readable storage for permitting access to a network protected behind a stealth firewall. Referring to independent claims 1, 8-9, and 12-13 and Figure 2 of Appellant's disclosure, a stealth firewall 210 is connected to an external network (left-side in Figure 2) via a first network interface and to a protected internal network 270 via a second network interface (page 12, lines 6-16 of Appellant's disclosure). The stealth firewall 210 includes a packet filter for restricting access to the internal network 270, in which the packet filter does not respond to the external network upon receiving requests 280 from the external network to access the internal network 270 (page 12, lines 18-20). Referring also to Figures 3A and 3B, the stealth firewall 210 includes a state machine 250 that is pre-configured to transition across a plurality of internal states, from a restricting state to an access state, conditioned upon receiving a plurality of requests 280 to access the internal network 270 (page 13, lines 3-9). The plurality of requests 280 collectively comprise a code for causing the state machine 250 to transition from the restricting state to the

access state which causes the packet filter to permit access to the internal network 270 (page 14, lines 1-7). As stated on page 14 of Appellant's disclosure "the state machine behaves analogously to a combination lock wherein the combination is comprised of the various values represented by Code 1, Code 2, …, Code n-1, Code n."

Referring to independent claims 7 and 11, a state machine 250 is initialized, and the state machine 250 is configured to grant access to the stealth firewall 210 contingent upon the state machine 250 transitioning across a plurality of internal states responsive to receiving a plurality of requests 280 to access the network 270 from a single network device 230 (page 13, lines 17-22). The plurality of requests 280 collectively comprise a code for causing the state machine 250 to permit access to the network 270 (page 14, lines 1-7). Referring also to Figures. 3A and 3B, once an access request 280 from a network device 230 has been received, an access parameter in the access request 280 is identified, and the state machine 250 is transitioned from an initial state to an intermediate state if the identified access request 280 satisfies transitioning criteria associated with the state machine 250 for transitioning from the initial state to the intermediate state (page 14, lines 1-4). A further access request 280 from the network device 230 is received and a further access parameter is identified in the further access request 280, which transitions the state machine 250 from an intermediate state to a final state if the identified further access request 280 satisfies transitioning criteria associated with the state machine 250 for transitioning from the intermediate state to the final state (page 14, lines 4-5). A response to the network device 230 is not provided upon receiving each of the access requests 280 from the network device 230 unless the network device 230 provides a sequence of access requests 280 to the stealth firewall 210 causing the state machine 250 to transition to the final state, which permits

the network device 230 to access the network 270 protected behind the stealth firewall 210 (page 12, line 18 through page 13, line 2; page 14, lines 5-7).

## VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

1. Claims 1-9 and 11-13 were rejected under 35 U.S.C. § 103 for obviousness based upon Rothermal et al., U.S. Patent No. 6,678,827 (hereinafter Rothermal), in view of Kikuchi et al., U.S. Patent No. 6,377,948; and

2. Claim 10 was rejected under 35 U.S.C. § 103 for obviousness based upon Rothermal in view of Wiser et al., U.S. Patent No. 6,868,403 (hereinafter Wiser).

## VII. ARGUMENT

### THE REJECTION OF CLAIMS 1-9 AND 11-13 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON ROTHERMAL IN VIEW OF WISER

For convenience of the Honorable Board in addressing the rejections, claims 2-6, 8-9, and 11-13 stand or fall together with independent claim 1, and independent claim 11 stands or falls together with independent claim 7.

Claim 1

Independent claim 1, in part, recites:

> a state machine pre-configured to transition across a plurality of internal states, from a restricting state to an access state, conditioned upon receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network.

To teach the claimed "preconfigured to transition across a plurality of internal states," the Examiner cited column 4, lines 35-45 and column 5, line 65 through column 6, line 2 of Rothermal, which for ease of reference are reproduced below:

> In particular, the Network Security Device Management (NSDM) system allows a security policy manager device to create a consistent security policy for multiple network security devices (NSDs) by distributing a copy of a security policy template to each of the NSDs and by then configuring each copy of the template with NSD-specific information. Other information useful for implementing security policies for the NSDs, such as software components to be executed by the NSDs or lists of devices from whom information is to be blocked, can also be distributed by the manager device to the NSDs in a similar manner. The NSDM system also allows a manager device to retrieve, analyze and display the network security information gathered by the various NSDs while implementing security policies. (column 4, lines 32-46)
>
> In addition, various schemes can be used to ensure that NSDs and supervisor devices provide information only to authorized devices or users, such as by using passwords, hashing passwords to produce keys, challenge/response, shared secrets, digital IDs, or a list of devices defined as being authorized to request and/or receive information. Part of the NSD-specific configuration of each NSD can include associating one or more supervisor devices authorized to communicate with the NSD, as well as providing specific information about how the communication is to occur. (column 5, line 61 through column 6, line 4).

Upon reviewing these cited passages, Appellant is entirely unclear as to what teaching within these passages discloses the claimed "transition across a plurality of internal states."

---

Claim 1 further clarifies that the transitioning of a plurality of internal states includes "from a restricting state to an access state," for which the Examiner cited column 15, lines 48-56 and column 13, lines 47-67 of Rothermal. The passage cited with regard to column 13 describes the architecture of the network security device (NSD), and the citation to column 15 describes the method illustrated in Fig. 8 of Rothermal, which describes packets being filtered based upon filter rules.

---

Independent claim 1, in part, further recites:

> said packet filter not responding to said external network upon receiving any request from said external network to access said internal network when said state machine in said restricting state.

To teach this limitation, the Examiner cited column 5, lines 39-51 and column 9, lines 28-39 of Rothermal. In this regard, Appellant respectfully submits that the Examiner's analysis is deficient as to this particular limitation.

Initially, Appellant notes that the two passages cited by the Examiner in columns 5 and 9 are completely unrelated to the claimed limitation for which these passages are being cited to teach. Both of these passages refers to "host supervisor devices," which "assist the manager device in retrieving, analyzing and displaying the network security information gather by the various NSDs" (column 5, lines 29-32). Referring to Fig. 2, Rothermal teaches that if a primary supervisory devices 120 is unable to host the network security information from NSD 130, alternate/secondary supervisory devices 160, 210 may be used to host the network security information. In essence, the cited passages of column 5, lines 39-51 and column 9, lines 28-39 are directed to teaching the forwarding of network information to other supervisory devices when a primary device is unable to receive the network information.

Moreover, Appellant notes that claim 1 recites that the packet filter does not respond to "any request to access said internal network" when the state machine is in the restricting state. The Examiner, however, has neither identified teachings within Rothermal as to requests for

access to an internal network nor as to all of these requests for access not being responded to in the restricting state.

---

With regard to the claimed "conditioned upon receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network," on page 4 of the Office Action, the Examiner admitted that Rothermal fails to teach or suggest this limitation. The Examiner did, however, assert that Rothermal generally teaches gathering network security information that is analyzed during the process of protection from unauthorized access.

As to the secondary reference of Kikuchi, the Examiner asserted the following on page 4 of the Office Action:

> Kikuchi [sic] an invention of transmitting and requesting access to documents on workstations through a network such as LAN (col. 1, lines 12-15). Kikuchi discloses receiving a request for accessing information and analyzing the contents of the access request where the sequence of issued access request are collectively reflected in the database as a single transaction (col. 4, lines 15-22). In addition, when the client issues a sequence of access requests, the consistence is guaranteed for a plurality of information items to be process [sic] by the access requests (col. 2, lines 62-65).

Initially, Appellant respectfully submits that Kikuchi is non-analogous prior art that cannot be applied against the claimed invention. Whether a prior art reference is from a nonanalogous art involves (a) determining whether the reference is within the same field of endeavor and (b) determining whether the reference is reasonably pertinent to the particular

problem with which the invention is involved.[1] If the prior art is outside the inventor's field of endeavor, the inventor will only be presumed to have knowledge of prior art that is reasonably pertinent to the problem being addressed.[2] The Examiner is also charged to consider "'the reality of the circumstances' … in other words, common sense" to determine what field a person of ordinary skill in the art would reasonably be expected to look.[3]

Whereas the claimed invention is directed to restricting access to an internal network from request received from an external network (i.e., related to network security), the teachings of Kikuchi are directed to "a method of reliably accessing data on a directory server in a network (column 1, lines 6-7), and is unrelated to network security. Thus, the claimed invention directed to network security and the teachings of Kikuchi are not within the same field of endeavor. Furthermore, the claimed invention is directed to, in part, solving the problem of how to prevent an unauthorized user from detecting the presence of a firewall (page 4 of Appellant's disclosure). In contrast, McCabe describes a method of guaranteeing consistency in directory information even if inadvertently interrupted due to a fault (column 2, lines 39-46). As Kikuchi is silent as to firewall or network security in general, common sense would dictate that Kikuchi is not reasonably pertinent to preventing an unauthorized user from detecting the presence of a firewall. Thus, the inescapable conclusion is that Kikuchi is non-analogous prior art that cannot be applied against the claimed invention.

---

[1] In re Clay, 23 USPQ2d 1058 (Fed Cir. 1992).
[2] In re Wood, 202 USPQ 171 (C.C.P.A. 1979).
[3] In re Oetiker, 977 F.2d 1443, 24 USPQ2d 1443 (Fed. Cir. 1992).

Notwithstanding that Kikuchi is non-analogous prior art, Kikuchi fails to teach or suggest the limitations for which the Examiner is relying upon Kikuchi to teach. Although Kikuchi teaches "a transaction processing unit 9 for processing a sequence of access request as a single transaction" (column 4, lines 19-21), Kikuchi fails to teach that this sequence of access requests "collectively comprising a code." Moreover, Kikuchi fails to teach that this sequence of access of requests "[cause] said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network." Still further, as noted above, Kikuchi is silent with regard to network security. As a result, Kikuchi is also silent as to a restricting state and an access state.

---

With regard to the requisite motivation to combine, the Examiner asserted the following in the paragraph spanning pages 4 and 5 of the Office Action:

> Hence, it would have been obvious for a person of ordinary skills in the art at the time of the invention to combine the method as taught by Kikuchi because by receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state guarantees for a plurality of information items to be processed, thus, can determine the restricting state to an access state of Rothermel [sic].

The Examiner's asserted motivation to combine in unpersuasive on several levels. The alleged benefit of "guarantees for a plurality of information items to be processed" doesn't describe what is being guaranteed (i.e., for the plurality of information items to be processed, what is being guaranteed?). Notwithstanding this omission by the Examiner, Appellant presumes that the Examiner intended to write "consistency," since the Examiner's alleged benefit appears to be derived from column 2, lines 61-65 of Kikuchi).

There is, however, no nexus between the missing limitation (i.e., "conditioned upon receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network") and the alleged benefit of guaranteed consistency. The guaranteed consistency taught by Kikuchi is a result of Kikuchi's method for providing access to data on a directory server in a network, which is unrelated to the claimed invention or the limitations not taught by Rothermal.

Moreover, Appellant notes that the Examiner's statement as to the motivation to combine, improperly asserts that Kikuchi teaches the missing limitation. As noted above, Kikuchi teaches processing a sequence of access requests as a single transaction, and not the claimed "conditioned upon receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network." Therefore, not only would one having ordinary skill in the art not be motivated to modify Rothermal in view of Kikuchi, even if one having ordinary skill in the art were motivated to combine the applied prior art, the claimed invention would not result.

Claims 7 and 11

Similar to independent claim 1, independent claims 7 and 11 recite the following claimed features: (i) a plurality of internal states; (ii) a restricting state; (iii) a plurality of requests to access an internal network; and (iv) an access state. Independent claims 7 and 11 also recite (v)

an intermediate state. In this regard, Appellant incorporates herein the arguments previously presented with regard to the limitations (i) through (iv).

As to the claimed "intermediate state," this limitation is found in the following limitation recited in claims 7 and 11:

> identifying an access parameter in said access request and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state.

To teach this limitation, on page 6 of the office action, the Examiner cited column 8, lines 59-60 and column 13, lines 47-67 of Rothermal. As discussed in detail above, Rothermal teaches that the NSD forwards network information to the additional supervisor devices if the primary device is unable to receive the network information. The Examiner's citation to column 8 only refers to "a variety of criteria," which is used to specify the additional supervisor devices for a particular NSD. As such, this passage is completely unrelated to the claimed limitation for which this passage is being cited to teach.

The second cited passage of column 13 is the same passage the Examiner cited above with regard to claim 1, and as already noted above, this passage describes the architecture of the network security device (NSD). Moreover, upon reviewing this passage, Appellant is unclear how this passages teaches any of the imitations for which this passage is being cited by the Examiner to teach.

With regard to the secondary reference of Kikuchi applied by the Examiner, Appellant incorporates herein the arguments previously presented with regard to claim 1 as also applying to claim 7. Moreover, Appellant notes that the Examiner has used the convention of placing [*claimed language in brackets and in italics*] when the primary reference of Rothermal fails to teach this language. Referring to pages 5 and 6 of the Office Action, the Examiner has identified several limitations in claim 7 via brackets and italics that are not taught or suggested by Rothermal. In comparison to the limitations recited in claim 1 not taught by Rothermal, considerably more limitations are identified in claim 7. However, what the Examiner has asserted as the teachings of Kikuchi and the motivation to modify Rothermal in view Kikuchi for claim 7 is identical to what the Examiner asserted for claim 1 (compare the last full paragraph on page 4 and the paragraph spanning pages 4 and 5 with the paragraph spanning pages 7 and 8 and the first full paragraph on page 8). These asserted teachings of Kikuchi and the Examiner's asserted motivation to combine, however, do not address many of the limitations the Examiner has identified as not being taught by Rothermal. Thus, the Examiner has failed to establish a prima facie case of obviousness.

Claims 8 and 12

Similar to independent claim 1, independent claims 8 and 12 recite the following claimed features: (i) state transitions; (ii) a restricting state (i.e., the claimed "not providing a response to said plurality of network device upon receiving each of said access states"; (iii) a plurality of requests to access an internal network; (iv) code for causing transitioning of states (i.e., the claimed "pre-determined sequence of access request parameters;" and (v) an access state (i.e., the claimed "permitting access"). In this regard, Appellant incorporates herein the arguments

previously presented with regard to the limitations (i) through (v). Appellant also incorporates herein the arguments previously presented with regard to the Examiner's asserted motivation to modify Rothermal in view of Kikuchi.

Claims 9 and 13

Similar to independent claim 1, independent claims 9 and 13 recite the following claimed features: (i) state transitions; (ii) a plurality of requests to access an internal network; (iii) code for causing transitioning of states (i.e., the claimed "a sequence of access request parameter identified in received access requests from a single network device;" and (iv) an access state (i.e., the claimed "grant access"). In this regard, Appellant incorporates herein the arguments previously presented with regard to the limitations (i) through (iv). Appellant also incorporates herein the arguments previously presented with regard to the Examiner's asserted motivation to modify Rothermal in view of Kikuchi.

**THE REJECTION OF CLAIM 10 UNDER 35 U.S.C. § 103 FOR OBVIOUSNESS BASED UPON ROTHERMAL IN VIEW OF WISER**

For convenience of the Honorable Board in addressing the rejections, claim 10 stands or falls alone.

On page 18 of the Office Action, Appellant presumes the Examiner intended to assert that "Rothermal [does not] go into details of a hash processor …", since the Examiner relied upon Wiser to teach these limitations. Upon reviewing Wiser, Appellant notes that Wiser is not directed to permitting access to an internal network in response to requests from an external

network. Instead, Wiser teaches mutual authentication between an authoring tool 102 and a content manager 112, which do not appear to be separated by a firewall. Therefore, even if Rothermal were modified in view of Wiser, the claimed invention would not result.

Conclusion

Based upon the foregoing, Appellant respectfully submits that the Examiner's rejections under 35 U.S.C. § 103 for obviousness based upon the applied prior art is not viable. Appellant, therefore, respectfully solicits the Honorable Board to reverse the Examiner's rejections under 35 U.S.C. § 103.

To the extent necessary, a petition for an extension of time under 37 C.F.R. § 1.136 is hereby made. Please charge any shortage in fees due under 37 C.F.R. §§ 1.17, 41.20, and in connection with the filing of this paper, including extension of time fees, to Deposit Account 09-0461, and please credit any excess fees to such deposit account.

Date: August 30, 2006

Respectfully submitted,

/s/ Scott D. Paul
Scott D. Paul
Registration No. 42,984
Steven M. Greenberg
Registration No. 44,725
CUSTOMER NUMBER 46320

## VIII. CLAIMS APPENDIX

1. A stealth firewall comprising:

a first network interface to an external network;

a second network interface to an internal network;

a packet filter for restricting access to said internal network; and,

a state machine pre-configured to transition across a plurality of internal states, from a restricting state to an access state, conditioned upon receiving a plurality of requests to access said internal network, said plurality of requests collectively comprising a code for causing said state machine to transition from said restricting state to said access state which causes said packet filter to permit access to said internal network, wherein

said packet filter not responding to said external network upon receiving any request from said external network to access said internal network when said state machine in said restricting state.

2. The stealth firewall of claim 1, wherein said requests from said external network comprise transport control protocol (TCP) SYN messages.

3. The stealth firewall of claim 2, wherein each state in said state machine corresponds to data in a specified field of said TCP SYN messages.

4. The stealth firewall of claim 3, wherein said specified field comprises a destination port field.

5. The stealth firewall of claim 1, wherein said code is a rolling code which can vary according to time.

6. The stealth firewall of claim 2, wherein said packet filter can permit access to a specific port in said internal network based upon a destination port specified in a TCP SYN message received after transitioning to said access state in said state machine.

7. A method for permitting access to a network protected behind a stealth firewall comprising the steps of:

initializing a state machine configured to grant access to the stealth firewall contingent upon said state machine transitioning across a plurality of internal states responsive to receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network;

receiving an access request from a network device in a network which is external to the network protected behind the stealth firewall, identifying an access parameter in said access request and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state;

receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access parameter in said further access request and transitioning from an intermediate state in said state

machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state;

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state; and,

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall.

8. A method for permitting access to a network protected behind a stealth firewall comprising the steps of:

receiving a plurality of access requests from a plurality of network devices which are external to the network protected behind the stealth firewall;

not providing a response to said plurality of network device upon receiving each of said access requests;

identifying access request parameters in said received access requests;

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; and,

upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters.

9. A method for permitting access to a network protected behind a stealth firewall comprising the steps of:

configuring a state machine to grant access to the stealth firewall contingent upon said state machine transitioning through a plurality of states based upon a sequence of access request parameters identified in received access requests from a single network device;

setting said sequence of access parameters to a specific set of access parameters; and,

disposing said state machine in the stealth firewall.

10. A stealth firewall comprising:

a first network interface to an external network;

a second network interface to an internal network;

a packet filter for restricting access to said internal network, said packet filter ignoring requests from said external network to access said internal network;

fixed storage in which at least one authentication password can be stored;

a hash processor configured to apply a hashing algorithm to said stored at least one authentication password; and,

a comparator configured to compare a hashed password and timestamp received from said first network interface, with a hashed result produced by said hash processor for a stored password associated with a user at said first network interface, said comparator causing said packet filter to permit access to said internal network where said hashed password and timestamp matches said hashed result.

11. A machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

initializing a state machine configured to grant access to the stealth firewall contingent upon said state machine transitioning across a plurality of internal states responsive to receiving a plurality of requests to access the network from a single network device, said plurality of requests collectively comprising a code for causing said state machine to permit access to the network;

receiving an access request from a network device in a network which is external to the network protected behind the stealth firewall, identifying an access parameter in said access request and transitioning from an initial state in said state machine to an intermediate state if said identified access request satisfies transitioning criteria associated with said state machine for transitioning from said initial state to said intermediate state;

receiving a further access request from said network device in said network which is external to the network protected behind the stealth firewall, identifying a further access parameter in said further access request and transitioning from an intermediate state in said state machine to a final state if said identified further access request satisfies transitioning criteria associated with said state machine for transitioning from an intermediate state to said final state;

not providing a response to said network device upon receiving each said access request from said network device in said network which is external to the network protected behind the stealth firewall unless said network device provides a sequence of access requests to the stealth firewall causing said state machine to transition to said final state; and,

upon transitioning to said final state, permitting said network device to access the network protected behind the stealth firewall.

12. A machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

receiving a plurality of access requests from a plurality of network devices which are external to the network protected behind the stealth firewall;

not providing a response to said plurality of network device upon receiving each of said access requests;

identifying access request parameters in said received access requests;

performing state transitions in a state machine in the stealth firewall based upon identifying particular ones of said identified access request parameters; and,

upon identifying a pre-determined sequence of access request parameters, said identification of said sequence of access request parameters causing a corresponding sequence of state transitions in the said machine, permitting access to a selected network device responsible for transmitting said sequence of access requests parameters.

13. A machine readable storage having stored thereon a computer program for permitting access to a network protected behind a stealth firewall, said computer program comprising a routine set of instructions for performing the steps of:

configuring a state machine to grant access to the stealth firewall contingent upon said state machine transitioning through a plurality of states based upon a sequence of access request parameters identified in received access requests from a single network device;

setting said sequence of access parameters to a specific set of access parameters; and,

disposing said state machine in the stealth firewall.

## IX. EVIDENCE APPENDIX

No evidence submitted pursuant to 37 C.F.R. §§ 1.130, 1.131, or 1.132 of this title or of any other evidence entered by the Examiner has been relied upon by Appellant in this Appeal, and thus no evidence is attached hereto.

## X. RELATED PROCEEDINGS APPENDIX

Since Appellant is unaware of any related appeals and interferences, no decision rendered by a court or the Board is attached hereto.